Exhibit A

EMV Payment Tokenization Primer and Lessons Learned

Version 1.0

Publication Date: June 2019

U.S. Payments Forum
191 Clarksville Road
Princeton Junction, NJ 08550

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum, formerly the EMV Migration Forum, is a cross-industry body focused on supporting the introduction and implementation of EMV chip and other new and emerging technologies that protect the security of, and enhance opportunities for payment transactions within the United States. The Forum is the only non-profit organization whose membership includes the entire payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on, and have a voice in the future of the U.S. payments industry. Additional information can be found at http://www.uspaymentsforum.org.

About the Mobile and Contactless Payment Working Committee

The Mobile and Contactless Payments Working Committee goal is for all interested parties to work collaboratively to explore the opportunities and challenges associated with implementation of mobile and contactless payments in the U.S. market, identify possible solutions to challenges, and facilitate the sharing of best practices with all industry stakeholders.

Table of Contents

1. Introduction

In payment processing, tokenization is the process of substituting sensitive data (e.g., payment card numbers and other personally identifiable Information [PII]) with a non-sensitive equivalent, referred to as a token, that has no extrinsic or exploitable meaning or value. The purpose of this is to minimize the risk of PII data fraud by rendering it useless.

While tokenization within the card payments industry takes various forms, this white paper was developed as a primer on payment tokenization as defined by EMVCo in the *Payment Tokenization Technical Framework*.[1] EMV payment tokens are valid for the entire lifecycle of a transaction and are now implemented in several payment channels, including payments made using Near Field Communication (NFC)-enabled mobile phones.

This white paper includes the following content:

- Definitions of the different forms of tokenization
- Scenarios for using EMV payment tokens across various channels
- Payment tokenization stakeholder roles
- Payment tokenization provisioning and processing flows
- Payment tokenization impact on merchants
- Lessons learned from implementing EMV payment tokenization as specified in EMVCo Payment Tokenization Framework, v1.0.

A number of topics were determined to be out of scope for this white paper, including:

- Implementation details applicable to other token types
- Tokenization challenges for specific merchant verticals
- Differences in tokenization with magnetic stripe data (MSD) and EMV contactless transactions
- Differences in tokenization with Magnetic Secure Transmission (MST) and NFC contactless transactions
- Details about implementation of token assurance method
- Merchant-initiated transactions and tokenization impact
- Tokenized card-on-file transactions that use cryptograms for domain control
- Payment Card Industry Data Security Standard (PCI DSS) requirements
- EMV Payment Account Reference (PAR) implementation
- Issuer, merchant, and acquirer settlement and reporting
- Impact on the process for exception management, disputes, chargebacks, and representments
- 'On-Us' transactions

Some of these topics may be covered in a future white paper.

[1] https://www.emvco.com/emv-technologies/payment-tokenisation/.

Additional information on tokens can be found in the U.S Payments Forum white papers *Mobile and Contactless Payments Requirements and Interactions* and *Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions*.[2]

[2] Available on the U.S. Payments Forum web site, https://www.uspaymentsforum.org/mobile-and-digital-wallets-u-s-landscape-and-strategic-considerations-for-merchants-and-financial-institutions/.

2. What Is Tokenization?

Tokenization substitutes placeholder characters or a surrogate, called a payment token, for the primary account number (PAN) in a financial transaction. As used in this paper, tokenization means replacing a PAN with a non-sensitive value that represents a card number for the purpose of payment processing. The tokenization service is offered by a token service provider (TSP), which is typically a payment network, an acquirer, a third-party service provider, or an issuer.

Tokenization protects payment data using a combination of techniques, such as secure storage of sensitive data or and/cryptographic controls, ensuring that an unauthorized party cannot mathematically reverse the token value to the original PAN. Token domain controls protect the token against unauthorized use.

Tokenization may use various format options for tokens, ranging from token values that are distinguishably different from the PAN to others that maintain some of the original digits of the PAN and look similar.

2.1 Types of Tokens

Two types of tokens are generally in use today: acquiring domain tokens (aka merchant or acquirer tokens) and payment tokens.

2.1.1 Acquiring Domain Tokens

Acquiring domain tokens were developed over a decade ago, as a solution to protect data at rest and as a way to comply with PCI DSS requirements. Many merchants use a tokenization service offered by their acquirer, and they are often intended to work with merchant processes such as return, loyalty, and analytics.

Some larger merchants create and manage their own tokens for a variety of reasons, including needing a PCI-compliant solution before acquirers had introduced such solutions, preserving independence from acquirers to allow for multiple acquirer relationships, and accommodating proprietary or closed-loop payment networks such as private label and gift cards.

An e- or m-commerce card-on-file (COF) token is a specific type of acquiring domain token that is used in online or mobile channels. COF acquiring domain tokens are typically unique to a particular channel and merchant.

2.1.2 EMV Payment Tokens

EMV payment tokens are open-loop tokens provisioned by a TSP and, like other tokens, are used to replace the actual payment credential (e.g., PAN) with another numeric value. Payment tokens may vary depending on implementation, but typically there is a unique token for each device, which bears no resemblance to the PAN (e.g., the final four digits do not match). They are used both for proximity contactless EMV transactions and, in some cases, for in-app transactions (e.g., Apple Pay). The same token value is used across all merchants.

Because tokens are typically unique to a device and channel, a single PAN can be represented by many tokens. For example, suppose Joe and Betty Smith share a credit card. That card can be represented by the following different tokens:

1. Joe's Apple Pay token in his iPhone
2. Joe's Apple Pay token on his Apple watch
3. Betty's Google Pay token on her Android device
4. Joe's e-commerce COF token with Merchant B
5. Betty's token with a pay button

2.2 Payment Tokenization Process

The payment tokenization process involves three primary participants: the token requestor, the TSP, and the payment card issuer. Each role performs different functions, as listed in **Figure 1** .

Figure 1. Participants in the Tokenization Process and their Associated Functions

The tokenization process includes nine major activities (Figure 2):

1. The issuer and token requester register with a token program.
2. The token requestor sends a provisioning request.
3. The issuer validates the card credentials and cardholder through an identity and verification (ID&V) process and sets the assurance level and any domain controls for the token.
4. The token is generated.
5. The token is provisioned and activated.
6. The cardholder uses the token in a payment transaction.
7. The token from the authorization message is detokenized and validated and the transaction is authorized.
8. The token is used to clear and settle the transaction.
9. The token is managed through its lifecycle.

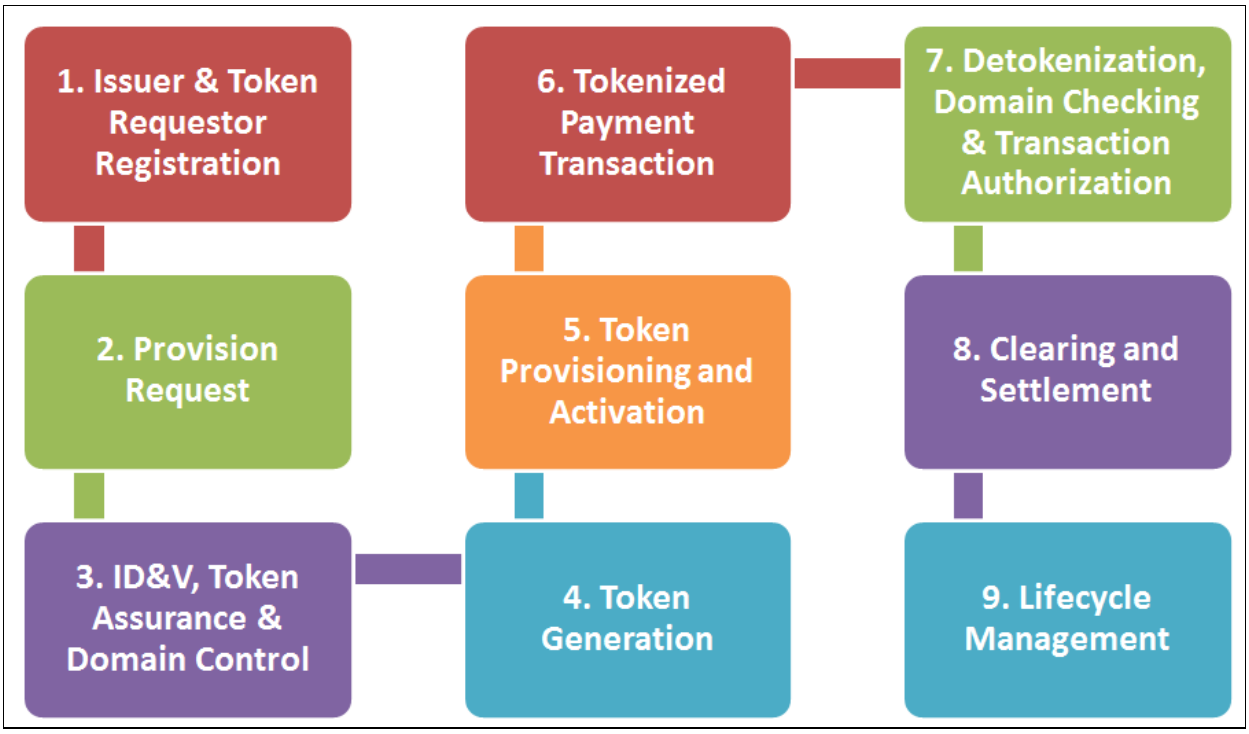


Figure 2. Overview of the Tokenization Process

2.3 Security in the Tokenization Process

Various measures provide security during the tokenization process.

2.3.1 Cryptography

Cryptography protects information by transforming it into a format only readable by authorized entities. Cryptography is often used to secure sensitive information, such as a PIN, or to authenticate an entity, such as an issuer or cardholder.

2.3.2 Token Cryptogram

Each transaction cryptographically generates a value that is unique to the transaction. This value is requested by the token requestor from the TSP, returned to the requestor, and used by the merchant in transaction processing.

2.3.3 Token Domain Restriction Control

Token domain restriction controls are a set of parameters that allow for the enforcement of appropriate usage of payment tokens during processing. The application of these controls provides the primary benefit of payment tokens and are intended to ensure that exposure of the payment token does not result in any significant fraud. Token domain restriction controls can be unique to the processing environment, the consumer's device or the token requestor. Examples include limiting use of the token to specific presentment modes, limiting use to a specific merchant and utilizing a token cryptogram. Token domain restrictions are administered by the TSP and the participating issuer.

2.3.4 Token Cryptographic Keys

As part of mobile wallets, static token keys are passed to the token requestor in order to generate the one-time token cryptograms for secure element implementations. The static key is provided one time during provisioning.

Wallet providers that use Host Card Emulation (HCE) to perform NFC-enabled contactless EMV transactions use limited use token keys, which are refreshed each time the user connects to a network.

Limited use token keys are generated by the master domain key and stored in a secure area of the mobile operating system, which uses software-based security, such as white box cryptography, to obfuscate the key. Limited use token keys generate cryptograms that are passed with the EMV payment token for each transaction.

Solutions using limited use token keys address the possibility that an Internet connection is not available to download a token. Transactions can be completed without network connectivity, because a token need not be requested from the cloud each time one is needed. Limited use token keys are restricted and expire quickly, minimizing their value to fraudsters.

2.3.5 Step-up Authentication during Identity and Verification (ID&V)

The ID&V process uses various methods for step-up authentication, including one-time passcodes (OTPs), call center support, app-to-app and email.

For example, certain transactions require a password or passcode that is valid for one login session or transaction only. When used in a registration process, an OTP verifies the user's e-mail address or mobile number by sending a verification code (the OTP) to the address or number during registration. OTPs prevent the user from registering with a fake e-mail address or mobile number. Upon successful entry of the OTP, the token is activated.

3. Tokenization Use Case Scenarios

Payment tokenization can be implemented in a variety of environments and use cases:

- In-store EMV contactless payments with device-centric[3] digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)
- In-app payments with device-centric digital wallets
- Card-on-file (COF) and recurring payments
- Pay button payments
- Payments made with wearables
- Payments made with Internet of Things (IoT) devices

The following sections provide an overview of each scenario; Section 5 includes additional details on each category of transaction.

3.1 In-Store EMV Contactless Payments with Device-Centric Digital Wallets

Apple, Google, and Samsung were among the first to implement EMV payment tokens in digital wallets that hold credentials for several payments use cases. These device-centric digital wallets play the role of a token requestor; they may capture the cardholder's PAN and request that it be replaced with a payment token from a TSP. Tokenization of payment credentials in digital wallets enables issuers to establish a secure presence on a wallet.

3.2 In-App Payments with Device-Centric Digital Wallets

In-app payments with device-centric digital wallets use a token that is already present in a digital wallet for checkout using a merchant's mobile app. In many cases, the digital wallet provider works with the merchant to enable the capability to pass the token during the transaction. In-app payments alleviate the need to enter payment card details, and other relevant information, manually into the merchant app while protecting the PAN.

3.3 Merchant Card-On-File and Recurring Payments

E-commerce merchants may store the customer payment credentials for use in recurring payments, installment payments, or on-demand purchases. Storing PAN information can create risk for merchants. Tokenization can mitigate these risks by replacing the PAN with a payment token, similar to the token used in a digital wallet. In this case, the merchant is the token requestor. Traditional e-commerce transactions are more secure when the TSP domain controls ensure that tokens are unique to each merchant and that transactions are secured with token cryptograms.

[3] See the U.S. Payments Forum white paper, "Mobile and Digital Wallets: U.S. Landscape and Strategic Considerations for Merchants and Financial Institutions," available at http://www.uspaymentsforum.org/mobile-and-digital-wallets-u-s-landscape-and-strategic-considerations-for-merchants-and-financial-institutions/, for additional information on different wallet models.

3.4 Pay Button Payments

Pay buttons are used by e-commerce sites in cases where the e-commerce merchant does not want to keep a card on file but still wants to take advantage of the security offered by tokenization. The button can tokenize the credentials, similar to the process that occurs when the customer uses a digital wallet. Pay buttons can enable tokens to be stored for multiple issuers and multiple payment network brands, and can also provide billing and shipping addresses to complete the checkout process. As in the in-app payment use case, consumers need not enter payment card information into the merchant app, and the PAN is protected where a token is provided.

3.5 Payments Using Wearables

Wearables are personal devices, such as fitness trackers, smart watches, clothing, or apparel, that are typically connected to the Internet through a separate WiFi- or Internet-enabled device. Wearables may or may not have a user interface and rely on a companion app that is resident on another mobile device (for example, a mobile phone with the app associated with a fitness tracker). This connectivity allows the wearable to be linked to a token requestor. Tokenization is facilitated through the app and then enabled for NFC transactions only. At present, tokenization provisioning and processing are typically the same as for device-centric digital wallets.

3.6 Payments Using the IoT

The IoT is a category of connected devices that expands beyond wearables to devices such as refrigerators or cars. Unlike wearables, IoT devices have direct network connectivity and may include a user interface. The connectivity and user interface facilitate both tokenization and e-commerce transactions. For example, a refrigerator may have a touch screen that can be used to order groceries. The payment credentials can be entered into the screen and tokenized for payments. Currently, IoT devices typically support e-commerce transactions. At present, tokenization provisioning and processing are typically the same as for merchant card-on-file transactions.

4. Payment Token Services

Implementing payment tokenization requires services for provisioning, processing, and managing tokens during a transaction. This section provides an overview of the services required by the tokenization ecosystem.

4.1 Issuer Enablement and Onboarding of Token Services

Issuers will select desired tokenization services based on a variety of available providers. Onboarding is required for the issuer to be enabled for the selected TSP.

This section will review a variety of onboarding options, wallet selections, token programs, configurations and settings that each TSP may choose to make available to issuers.

Issuer enablement activities include:

- Selecting general onboarding parameters
- Identifying wallet or token requestor programs
- Identifying account ranges
- Configuring programs

4.1.1 Onboarding Parameters

General onboarding parameters include:

- The country where the issuer wants to enable tokenization
- Issuer call center contact numbers
- Bank Identification Numbers (BINs)
- Card program identifier (debit or credit card)
- The transaction types to be supported, such as international cashback and domestic cashback

4.1.2 Wallets and Token Requestor Programs

TSPs will offer issuers participation in digital wallets and token requestor programs. Digital wallets can be from third-party providers in the ecosystem or be developed by the issuer. Token programs can be for devices, Internet of Things (IoT), or card-on-file.

During the issuer's onboarding to the TSP, participation in wallets and token requestor programs may be optional or pre-configured.

4.1.3 Account Ranges

As part of the onboarding process, issuers must identify what account ranges are available for tokenization for each wallet application or token program. Each account range is a series of PANs within a BIN. Issuers can specify multiple account ranges with gaps, if they want to exclude certain ranges. Once enabled by the issuer, all cards with PANs within the specified ranges can be tokenized by the relevant programs. Cards outside those ranges cannot be tokenized by those programs.

4.1.4 Program Configuration

A key TSP role is to act as the digital equivalent of the issuer's card personalization and embossing partner, traditionally played by others in the ecosystem for physical cards. As part of provisioning, TSPs may need to provide configuration assets such as pre-personalization data, EMV payment application identifiers (AIDs) and payment keys to devices and token requestors.

These configured assets are provided by issuers to TSPs during onboarding to represent the card in the digital space. The program configuration assets are then provided to token requestors during tokenization.

Examples of configuration assets include the following, but are further defined by the TSP and associated payment network(s):

- Digital card images – the digital representation of the account tied to the PAN. Some digital wallets require the image to look exactly like the physical card providing continuity to the consumer.
- Mobile banking application URL – link into a mobile banking app. Many digital wallets allow for issuers to link directly into a banking app to extend the experience to the issuer brand. For example, the consumer may be looking into transaction details starting in the wallet and then linking directly into the issuer's mobile banking app.
- Program names and product descriptions – consumer-facing descriptors that provide further continuity from physical to digital.
- Cardholder terms and conditions – issuer updated terms for usage with token requestor program.
- Authorization parameters – payment network options including options impacting the experience at the POS, such as the Cardholder Verification Method (CVM) list, cashback, authorization stand-in, and other network options.
- Tokenization messages for ID&V and detokenization – message options for the issuer (e.g., API, account status inquiry, enhanced network message, and others).
- TSP rules – on-behalf service rules for decisioning on the issuer's behalf by the TSP.
- Path default decisions – token request exception path default decision, if the issuer or network cannot respond.

4.2 Common Token Service Provider Services

Figure 3 shows the services that are commonly provided by a TSP. Individual TSPs may offer their token requestor customers some or all of these services, and the token requestors can choose which services they want as part of the onboarding process.

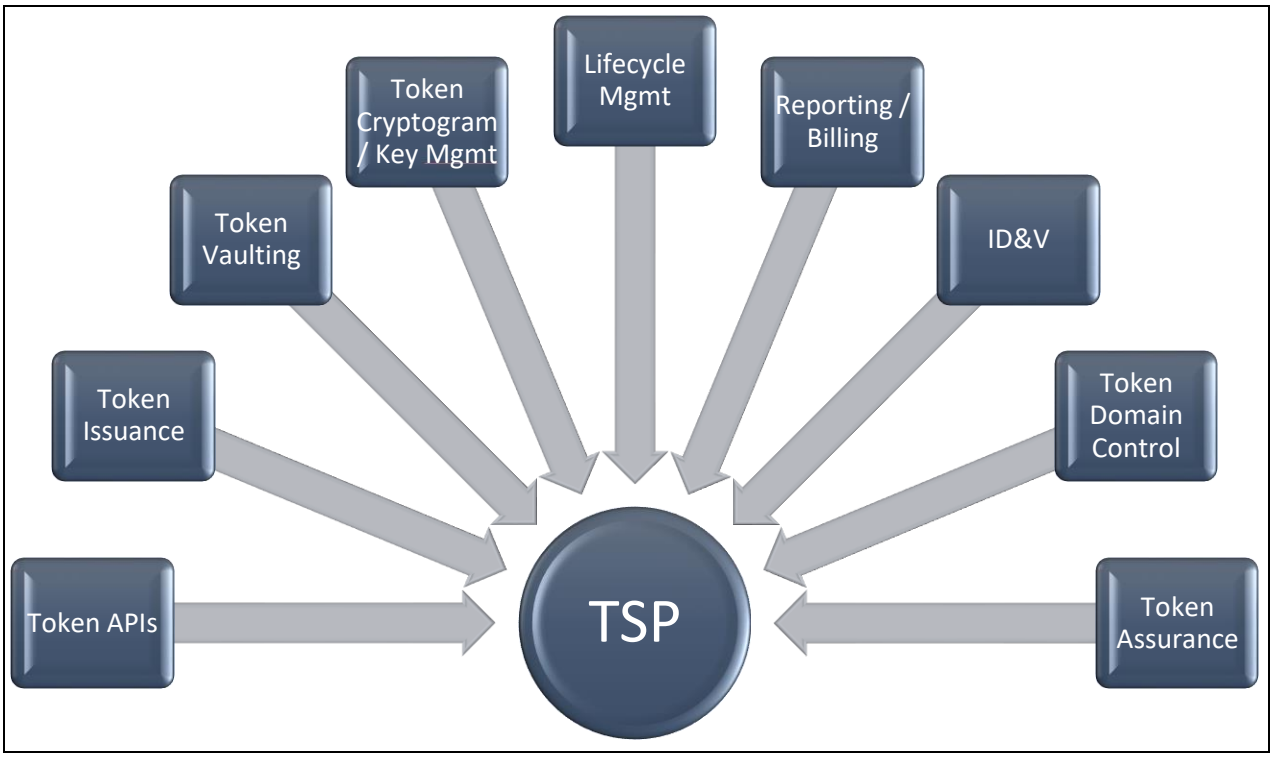


Figure 3. Overview of Services Commonly Provided by a TSP

4.2.1 Token APIs

Token vaults and TSPs interface with token requestors over an application programming interface (API) which facilitates tokenization and lifecycle management. Issuers use provisioning APIs to receive and respond to tokenization requests and manage the ID&V process. Using APIs facilitates flexibility with processing partners.

APIs also support customer service. Cardholders can manage their devices and cards (e.g., lost device or card deletion), that may result in lifecycle changes. It is critical that token requestors and issuers have the tools to manage tokens based on cardholder activity. (Token lifecycle management is described in Section 4.2.5.)

For some wallets and token requestors, a transaction history API is available to issuers and transaction processing partners. This API allows the transaction history to be displayed to the token requestor.

4.2.2 Token Issuance

Token issuance refers to the process by which tokens are created and distributed. Currently, payment networks and TSPs are typically responsible for token issuance. The process starts with onboarding the issuer's account range and ends when the TSP matches that range with a token range. As a part of provisioning an individual account or PAN, the token service generates a token, maps it to the PAN, and sends it to the token requestor. The vaulting service (Section 4.2.3) maintains the relationship between the PAN and the token.

Token issuance also includes the delivery of the newly created token. The TSP acts as a trusted service manager (TSM) delivering the token over the air or over an Internet connection to a device or merchant. The token is delivered using the token requestor API (Section 4.2.1).

4.2.3 Token Vault Service

A token vault is a secure centralized server where issued tokens, and the PAN numbers they represent, are stored securely. The token vault facilitates requests between the token requestor or merchant and issuer of the PAN. Once the token is created and stored in the TSP vault, authorizations will be generated and routed as normal, using TSP vault services. Vault services can include token issuance, key management, cryptogram validation, and domain controls.

4.2.4 Token Cryptogram and Key Management

One primary function of the TSP is to act as the TSM and deliver tokens and associated EMV-based payment applications to token requestors. The delivery and coordination of the keys with the token requestor (either a mobile device manufacturer or a merchant for an online payment) ensures that an EMV-compliant set of transaction data is generated. Transactions are routed to the TSP providing the validation service to validate the cryptogram before going to the issuer for authorization. Depending on the options selected by the issuer, the TSP may reject the transaction if cryptogram validation fails.

4.2.5 Lifecycle Management

Once a token is created, any changes to the PAN, token, device, or cardholder need to be controlled and updates sent through the tokenization ecosystem. The TSP makes access to the token lifecycle available to the issuer and token requestor and is responsible for notifying all parties of lifecycle changes. The token lifecycle is represented by different states. The TSP decides what activities are permitted in each state of a token's lifecycle, and the lifecycle state may be subject to some level of token domain control.

The token lifecycle and its expiration do not have to mirror the lifecycle and expiration of the PAN that token represents. A token can be suspended while the PAN is active. A PAN can expire but still be tokenized with an expiration date in the future.

Each individual issuer and TSP determine how to manage each lifecycle state. The lifecycle and the relationship between the PAN and the token can be managed using tools available from the TSP or network and an account updater tool, TSP API, or online network message.

4.2.6 Reporting

Token reporting can be provided by either the TSP or a partner with access to the token data. Reports typically provide historical data on the PAN or token volume, token transaction volume, current enablement, or lifecycle status. Refer to the EMVCo *Payment Tokenization Technical Framework* for additional details on reports.

4.2.7 ID&V

Before a token can be created and provided to a token requestor, the issuer of the PAN must authenticate the cardholder and approve tokenizing the account through the identification and verification (ID&V) process. The ID&V process typically has three stages: request, verification, and outcome. The decision paths are typically identified by a color.

- A green path indicates that token creation has been approved. The token is created in an active state and is ready to be used for payment.
- A red path indicates that the token request is declined. No token is created. There may be a variety of reasons that issuers decline a request, such as card balance or card status. The TSP and issuer may allow additional requests to be made.
- A yellow path indicates that the cardholder is subject to additional authentication requirements (called stepped-up authentication). The issuer provides the cardholder with actions to perform to verify the cardholder's identity and activate the token.

ID&V focuses mainly on the yellow path and cardholder options for resolution and token activation. The resolution options are driven by the capabilities of the token requestor, the TSP, and the issuer, and by available cardholder data. Common resolution options are:

- Call center. The cardholder calls the issuer's customer service line. The issuer customer service agent confirms the cardholder's identity and activates the token.
- Mobile phone text message. The cardholder may choose to receive a text message containing an activation code (to be entered into a wallet) that then activates the token.
- Cardholder e-mail message. The cardholder may choose to receive an e-mail message containing an activation code (to be entered into a wallet) that then activates the token.
- Issuer mobile banking app. The issuer may develop an app for mobile phones that allows the cardholder to log in with an ID and password controlled by the bank. Once logged in, the cardholder can activate the token in the wallet.

Issuers choose which options to make available to each cardholder. Options may be limited if the issuer does not have an e-mail address or a phone number that receives text messages for the cardholder. In addition, some of the options are complex and require developing software, such as the mobile banking app.

4.2.8 Token Domain Controls

Domain controls enforce appropriate token use on the basis of a set of parameters. The TSP invokes token controls based on the selected parameters and can decline authorization attempts. For example:

- Point-of-service entry. Is this a contactless transaction, an online transaction, or a COF transaction?
- Token requestor. Does this token belong to this token requestor?
- Recurring transaction. Is this transaction recurring, and is it identified appropriately?

4.2.9 Token Assurance

Token assurance is the process of ID&V that is part of payment tokenization. With the release of version 2.0 of the EMVCo Payment Tokenisation Specification – Technical Framework, the concept of token assurance level was revised to the token assurance method. Given this change, a future version of this paper will address token assurance once there is adequate experience with token assurance method.

4.3 Token Lifecycle Management

Figure 4 illustrates the potential stages in the lifecycle of a token.

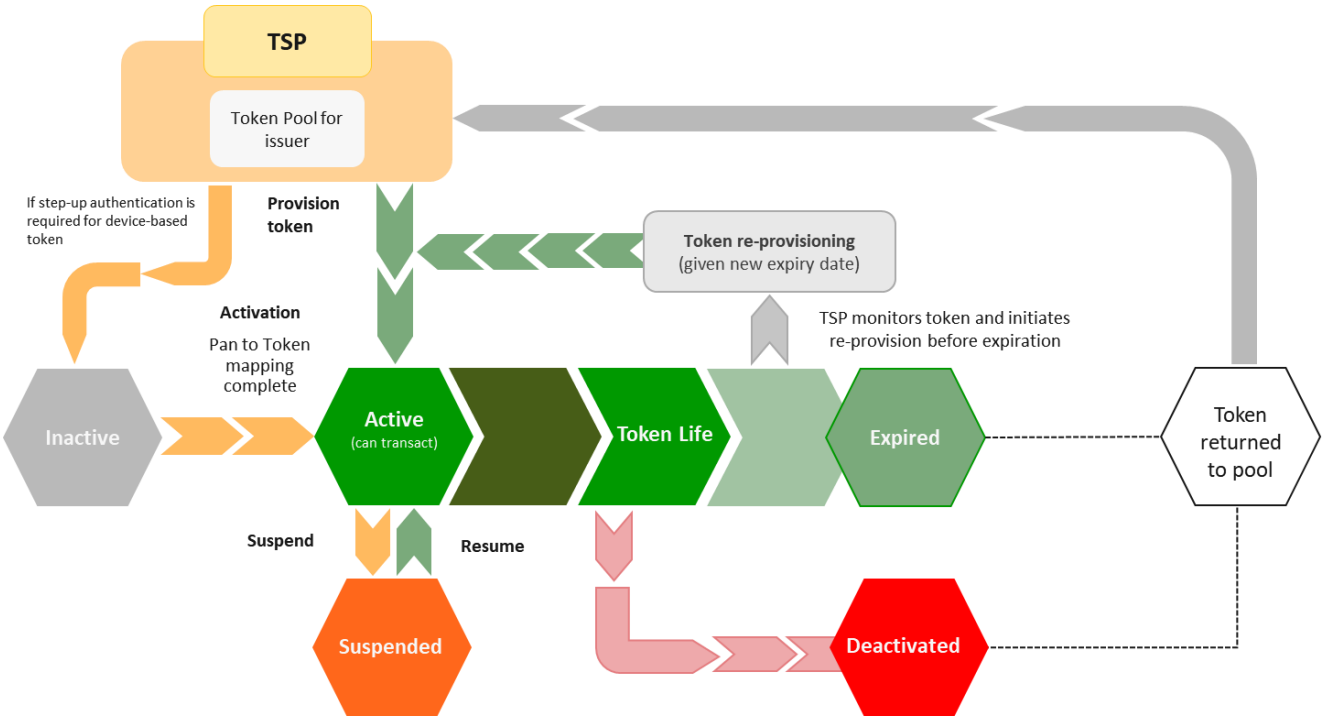


Figure 4. Lifecycle Stages of a Token and Token Status

Token lifecycle management is critical to the success of a wallet or card-on-file token solution. The PAN must remain associated with all appropriate tokens to ensure the best user experience. This relationship is managed by the TSP, which allows tokens and PANs to have independent lifecycles.

Tokens and the plastic card or other form factor associated with a single PAN should also be managed independently, so that changes to one do not affect the other. Changes to a particular token, such as token suspension or resumption of active status, do not need to impact all tokens associated with the PAN. Likewise, changes to the plastic card, such as an expiration update or reissuance, do not need to impact the tokens.

Various methods can be used to manage token lifecycles, depending on the payment network and issuer implementation. Issuers can use tools from the payment networks to update the token vault manually. Web service APIs can also be used, or enhanced network messages. In addition, certain PAN lifecycle updates can be made through other services, such as account updater services. Issuers should check with the payment network to determine the best method to use for token lifecycle management. They should consider factors such as the size of their card base and the availability of resources to keep up with changes to various APIs, files, and messages.

In addition, customers can perform token maintenance within the wallet applications (for example, removing the card/token from their wallet).

4.3.1 Token Status

The token lifecycle includes different token statuses (Figure 4). Actions taken while managing a token's lifecycle can change a token's status. The token's status determines that token's functions, capabilities, or limitations.

Five potential token statuses are:

- Inactive
- Active
- Suspended
- Deactivated[4]
- Expired

Each token vault or payment network has its own definition of the different token statuses. Following is a general description of each potential status.

Inactive is a pre-tokenization status. Inactive is typically assigned while creating a token, usually while mapping the token to a funding PAN or delivering the token to a token requestor. The token number may not be assigned or available to the token requestor or device and cannot be used for payments.

Active identifies a token that is mapped to a funding PAN and ready to be used for transactions. The token can be used for NFC, e-commerce, in-app, m-commerce, and COF authorizations and to create cryptograms. After successful ID&V, the token is generally moved to an active state.

A once-active token that the cardholder or issuer puts on hold is *suspended*. Transactions using this token are typically declined by the token vault service and returned to the merchant or acquirer. A suspended token can resume active status.

Deactivated identifies the end state of a token. Although the token may not be removed from the token vault service, it typically is removed from the token requestor's device or server. A token in this state cannot be reactivated, and all transactions using the token are declined by the token vault service.

Tokens, like PANs, have an expiration date. *Expired* tokens may be deactivated, although they may remain on the token requestor's device. Tokens that expire typically are not used again and remain unusable for transactions in a deactivated state. There is an option for TSPs to re-use these expired tokens after an appropriate amount of time allowing for clearing, chargeback and dispute processes to complete. This process ensures that a TSP's available pool of token numbers is not depleted. Another way to extend the life of a token and reduce the depletion of useable tokens is by re-provisioning the token.

Re-provisioning is intended provide an uninterrupted consumer experience and ability to transact. The token vault service can provide a method of re-provisioning the token with the same token number and a new expiration date. Otherwise for a consumer to continue to transact the token requestor can prompt the cardholder to re-provision, resulting in a new token number.[5] In the background and not through any interface with the consumer, a TSP may monitor the expiration date of a token and as the date nears, initiate a re-provisioning with the token requestor. The result is that the token's expiration

[4] Another term that is used is "unlinked" where the payment token is disconnected from the PAN and the mapping is disabled for further use.

[5] Note that token recycling is possible, based on a feature of the BIN owner. Token vaults typically allow for all related transaction, chargeback, and dispute processes to complete before considering reuse of a token. The amount of time involved may vary by payment network and is typically intended to allow enough time to complete any chargeback and settlement activity.

is updated without changing the token number and the token remains in an active status without expiring.

4.3.2 Impact of Lost/Stolen Cards or Devices or Theft Mitigation

The use of tokenization mitigates the risk of fraudulent transactions associated with lost or stolen cards or devices.

If a card is lost or stolen, there is no need to delete any existing tokens if there is no fraud associated with its token; the issuer would send a new plastic card and automatically update the token vault. If the device is lost or stolen, the token is deactivated and the card does not need to be replaced. In the case of a fraudulent tokenized transaction, the issuer customer support agent manually deactivates the associated token using the life cycle management tools. In addition, a new card is sent, and the token vault is automatically updated for all other tokens associated with the card. When a device is lost, the tokens for the PAN that are associated with that device in the payment network tools are deleted.

Updates can be made automatically using a tool provided by a network.

If there is a reissuance, product change, or mass compromise event, a new plastic card is sent, and the token vault automatically updated using one of the methods mentioned above. In the case of a derogatory account status (i.e., credit revoked, account closed or charged off), all tokens associated with the PAN can be deleted automatically if the issuer wishes.

Card art in a wallet may or may not update automatically, depending on the payment network and wallet. The customer may need to reprovision to show a new card image.

4.4 Third-Party Token Services

Third-party TSPs generally follow the same major use cases described in Section 4.2. To enable these use cases, third-party TSPs are generally composed of the following core modules:

- Customer management platform
- Token vault and provisioning platform
- Transaction processing system

4.4.1 Customer Management Platform

The customer management platform (CMP) is an onboarding platform used for issuer and token requestor registration and profile management. The CMP performs the following functions:

- Manages the rules for token domain restriction controls and ID&V methods
- Supports BIN management for tokens and PANs for the participating entities
- Manages product attributes such as terms and conditions and card art for token portfolios to enable provisioning and processing tokens
- Provides the customer service interface for manual token lifecycle management
- Provides audit and reporting abilities

4.4.2 Token Vault and Provisioning Platform

The token vault is the heart of a TSP and performs the following functions:

- Generates tokens and maps tokens to PANs, based on the rules defined for each token requestor and issuer
- Maintains multiple participating entities, and employs the security controls mandated by the payment networks and relevant industry standards
- Ensures access only to appropriate interfaces and participants to enable token issuance and token transaction processing
- Assigns token assurance levels based on the ID&V rules defined as part of enrollment
- Services detokenization requests during transaction processing and lifecycle management
- Supports cryptogram validation and domain restriction controls defined for a particular token BIN, as defined during registration
- Provisions tokens to the token storage location using one of the interfaces defined between the vault and token requestor.

4.4.3 Token Processing System

The token processing system can be a combination of the core TSP system and existing payment transaction processing platforms. This system is responsible for routing tokenized transactions to appropriate entities within and outside of the core TSP system. Entities could include authorization channels and capture, clearing, and settlement systems. Third-party TSP processing systems support multiple payment networks and token requestor and issuer combinations.

4.5 Token Vault Connectivity

In addition to the secure storage and mapping of tokens and PANs, the token vault facilitates tokenization requests, passing data between the token requestor or wallet provider and the issuer.

Token vaults provide the ability to provision tokens to devices via TSMs or other provisioning systems. Credentials are transported in secure data packages to provision into devices' secure storage locations such as secure elements or the secure memory area that is designated for payment credential storage.

Currently, TSPs focus on direct connections to token requestors, who may be the device manufacturers, COF merchants or payments partners who support merchants. These communications are made secure over shared networks, (i.e., the Internet using technologies such as encrypted messaging, APIs, and VPNs) and/or with dedicated connections (e.g., leased lines or private lines).

4.6 Token Requesting Gateways

Currently, a merchant who wants to support EMV payment tokens in the U.S. market may need to connect to four or more payment networks, which means integration with four or more TSPs. To provide a common integration, token gateways (or aggregators) are becoming desirable.

The payment networks have enabled certain companies to become tokenization gateways. Merchants, issuers, and service providers can all access the same services or use cases offered by a TSP through the gateway. The service integrates with multiple TSPs from different payment networks. Use of token gateways is growing. Such use not only simplifies integration for the issuer or merchant, it also allows the payment networks to reduce their issuer or merchant onboarding workload, which is especially important when TSPs consider scaling globally.

5. End-to-End EMV Payment Tokenization Flows

This section details the process flows for several of the following customer-initiated EMV-payment-token use-case scenarios (described in Section 3):

- In-store EMV contactless and in-app payments with device-centric digital wallets (e.g., Apple Pay, Google Pay, Samsung Pay)
- Merchant card-on-file payments
- Network pay button payments at e-commerce sites

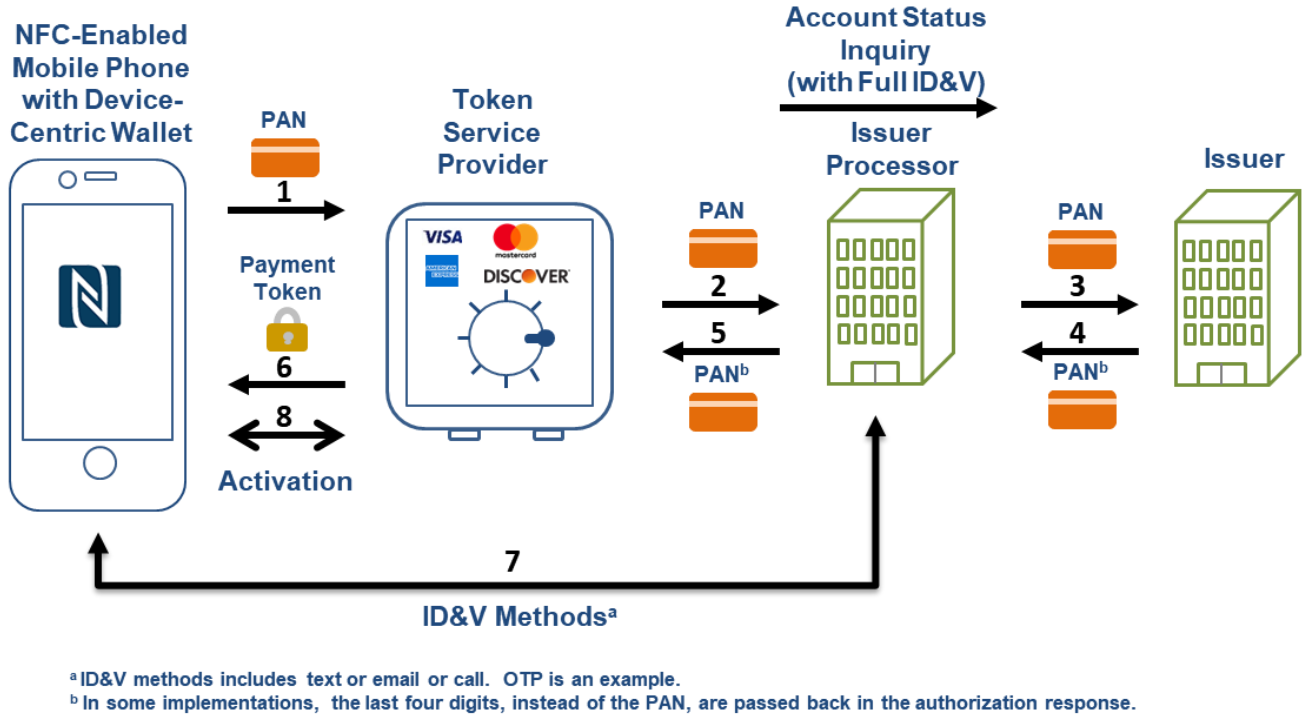
The flows below assume that the TSP shown supports all of the services discussed in Sections 2 and 4. There are implementations in market that separate functions among more than one entity.

5.1 Device-Centric Wallet Payments

Provisioning and transaction processing for mobile wallet transactions vary based on the type of mobile wallet used for the transaction.

5.1.1 Provisioning to Device-Centric Wallets

Figure 5 illustrates the token provisioning process for transactions that use an NFC-enabled mobile phone with a device-centric digital wallet.



[a] ID&V methods includes text or email or call. OTP is an example.
[b] In some implementations, the last four digits, instead of the PAN, are passed back in the authorization response.

Figure 5. Token Provisioning for an NFC-Enabled Phone with a Device-Centric Wallet

During provisioning, the following steps occur:

1. When the cardholder initiates a request to register a card, the digital wallet application issues a request to the TSP to enroll and provision the card.

2. The TSP creates an inactive token corresponding to the card and an OTP. The TSP then initiates an ID&V request to the issuer processor for the BIN associated with the card. For many networks, the request may be an account status inquiry request.

   ID&V methods include a text message to the cardholder's registered phone number, an e-mail message to the cardholder's registered e-mail address, or a phone call from the issuer to the cardholder or the cardholder to the issuer. See also steps 6 and 7.

3. The issuer processor completes the request by forwarding it to the issuer or financial institution (or performs on behalf of) for verification of the card credentials.
4. The issuer, or issuer processor on behalf of the issuer, approves the card verification or account status inquiry request and responds to the issuer processor.
5. The issuer processor propagates the approved response to the TSP.
6. The TSP responds to the digital wallet application, which in turn displays a "step-up" authentication dialog to the device or card owner.
7. Meanwhile, the issuer processor relays the OTP in the provisioning request to the cardholder over e-mail or a text message (as registered by the cardholder).
8. The cardholder enters the OTP into the step-up authentication dialog displayed in the digital wallet, which in turn sends the OTP to the TSP. The TSP then compares the OTP provided with the OTP generated, and successfully completes the provisioning and activates the token.

5.1.2 Transaction Processing (POS Contactless, Device-Centric Wallet)

Figure 6 illustrates the processing for in-store EMV contactless transactions using an NFC-enabled mobile phone with a device-centric digital wallet at a POS.

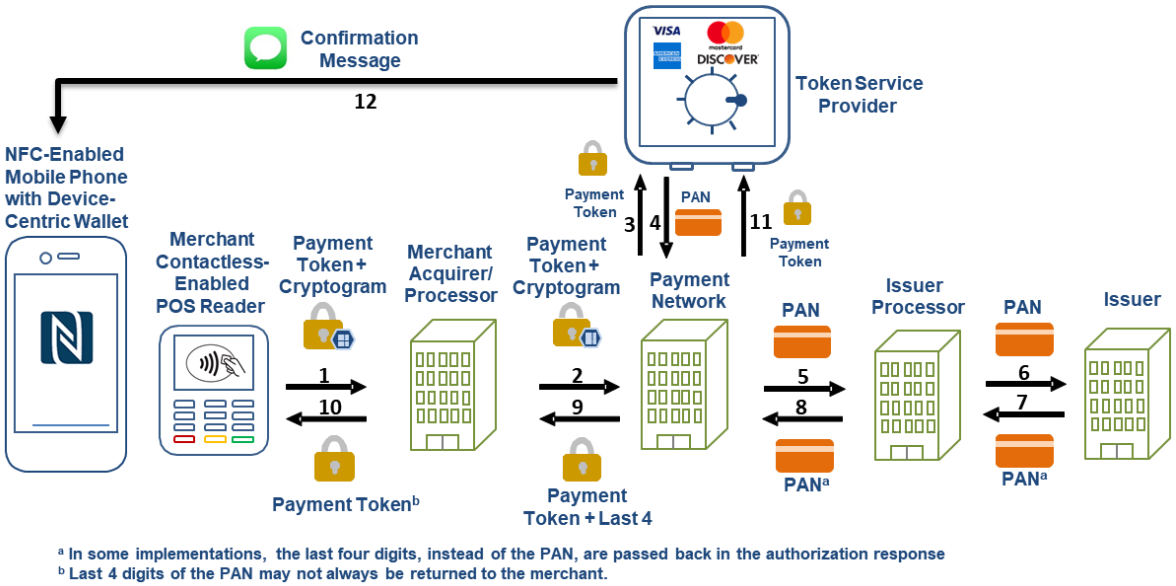


Figure 6. Processing a Contactless EMV Transaction Using an NFC-Enabled Device-Centric Digital Wallet

During the transaction, the following steps occur:

1. The cardholder taps a contactless-enabled mobile device at a merchant contactless POS device to pay for goods and services. A transaction authorization is initiated, and a corresponding message is sent to the merchant acquirer/processor containing the payment token from the cardholder's mobile device, along with a unique cryptogram.
2. The merchant acquirer/processor receives the transaction request, uses the token (looks like a PAN) to perform a token BIN lookup, and determines the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the PAN.
4. The TSP verifies the cryptogram and returns the clear PAN[6] to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the contactless terminal to complete the transaction. Meanwhile, the issuer processor sends a transaction completion notification, with the token, to the TSP, indicating the outcome of the transaction.
11. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process. Whether this step occurs depends on issuer participation.

5.1.3 Transaction Processing (In-App, Device-Centric Wallet)

Figure 7 illustrates the processing for in-app transactions using a merchant mobile app with tokens provisioned in an NFC-enabled mobile phone with device-centric digital wallet.

[6] Note that not all Track 2 discretionary data is provided to the issuer with the clear PAN, which could have implications for issuer verification.

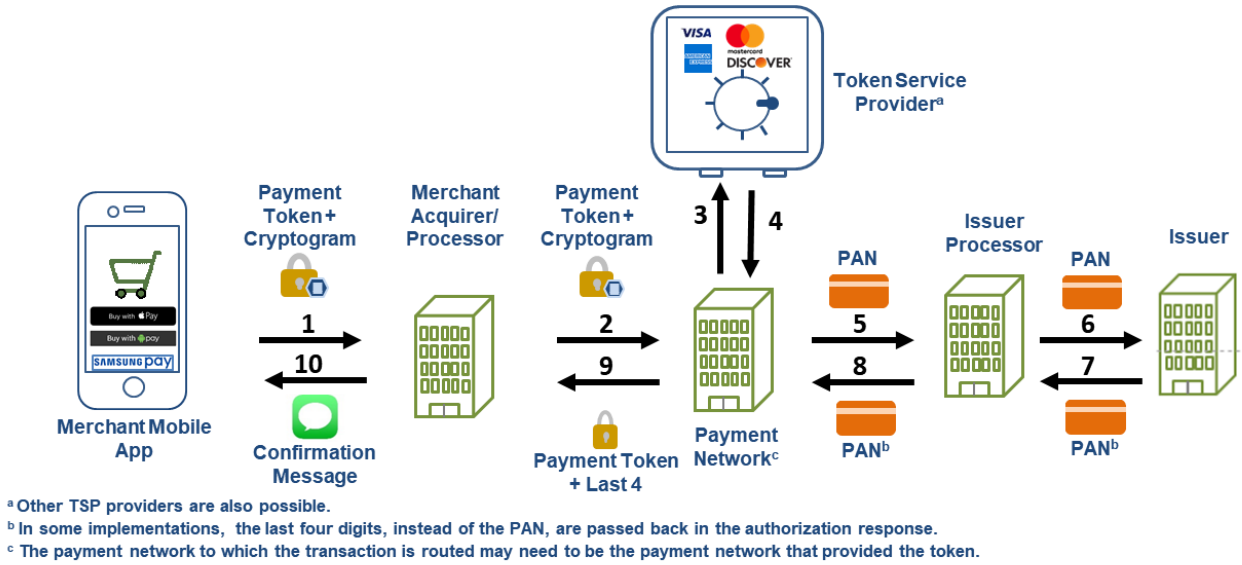


Figure 7. Processing an In-App Transaction Using a Merchant Mobile App with Tokens Provisioned in a Device-Centric Wallet

During the transaction process, the following steps occur:

1. The cardholder using the merchant mobile application selects to pay using an embedded mobile wallet (Google Pay/Apple Pay/Samsung Pay). The mobile application interacts with the native mobile wallet API to initiate payment with a list of accepted payment brands. The mobile wallet verifies that a token is available for the requested payment brand. If a token is available, the mobile wallet displays the default payment token. The cardholder verifies the amount and selects the token for payment. The mobile wallet authenticates the user with a biometric factor, PIN or passcode, and returns a payment token with a cryptogram to the mobile application. The payment token is sent to the merchant acquirer/processor in the authorization request.
2. The merchant acquirer/processor decrypts the encrypted payment token. The merchant acquirer/processor uses the token (looks like a PAN) to perform a token BIN lookup and determine the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to the clear PAN.
4. The TSP verifies the cryptogram and returns the clear PAN to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.

9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the mobile application with the transaction response. The TSP pushes a notification to the mobile device on which the token was initially provisioned during the enrollment process.

5.2 Merchant Card on File (COF)

Different processes are applicable at e- and m-commerce merchant sites that use stored cards.

5.2.1 Provisioning Process (Merchant Card on File)

Figure 8 illustrates the token provisioning process for transactions at a merchant shopping site that stores cards for future use.

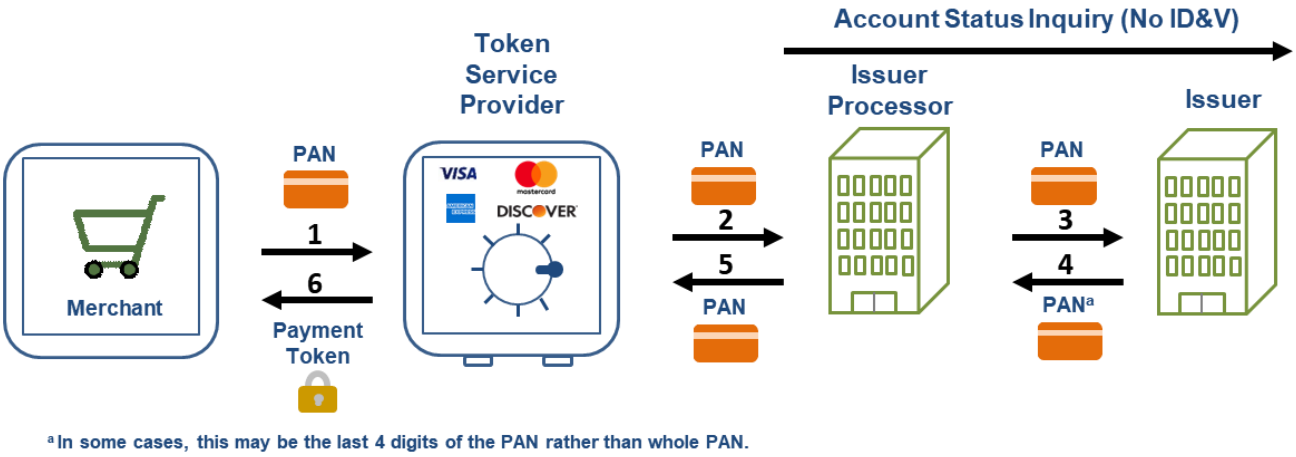


Figure 8. Token Provisioning at Merchant Sites that Store a Card (Card on File)

During provisioning, the following steps occur:

1. The cardholder elects to store a card for future use at merchant shopping site/mobile application. The merchant requests the TSP to tokenize the card.
2. The TSP validates the card or token with the issuer processor.
3. The issuer processor completes the request by forwarding it to the issuer/financial institution (or performs on-behalf-of) for verification of the card credentials.
4. The issuer verifies the card or account status and responds to the issuer processor. The card verification may include attributes such as lost/stolen.
5. The issuer processor sends the approved response to the TSP.
6. The TSP responds to the merchant with a token for future transactions.

5.2.2 Merchant COF Transaction Processing: American Express, Discover, Mastercard or Visa TSP

Figure 9 illustrates the transaction process when a stored tokenized card on file is routed to the American Express, Discover, Mastercard or Visa payment networks. Note that in some situations, a cryptogram may also accompany the token during transaction processing for domain control.

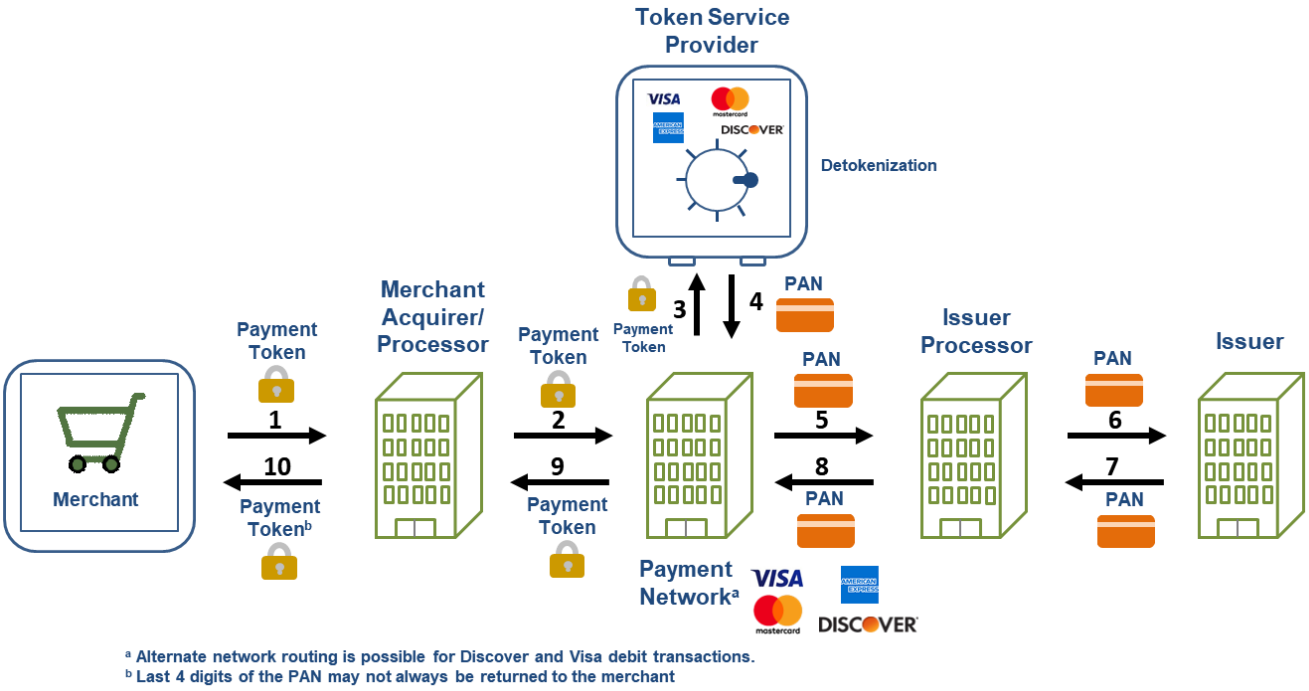


Figure 9. Process for Transactions Using a Merchant-Stored Tokenized Card (COF) Based on American Express, Discover, Mastercard or Visa TSP Tokens

During the transaction process, the following steps occur:

1. The cardholder at a merchant shopping site (or using a mobile application) elects to pay with a card previously stored on the merchant site. The transaction is initiated, and a message containing the payment token is forwarded to the merchant acquirer/processor.
2. The merchant acquirer/processor receives the transaction request and uses the token to perform a token BIN lookup and determine the networks to which the transaction can be routed. Based on the presence of the token, the merchant acquirer/processor may only be able to route the transaction to the payment network associated with the TSP.
3. The payment network determines that the transaction is based on a token BIN and issues a request to the appropriate TSP detokenize the token to the clear PAN.
4. The TSP returns the clear PAN to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.

7. The issuer completes authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the merchant's web site or mobile application to complete the transaction.

5.2.3 Merchant COF Transaction Processing: Third-Party TSP

Figure 10 illustrates the process for transactions using a stored tokenized card using a third-party TSP (not tied to any payment network).

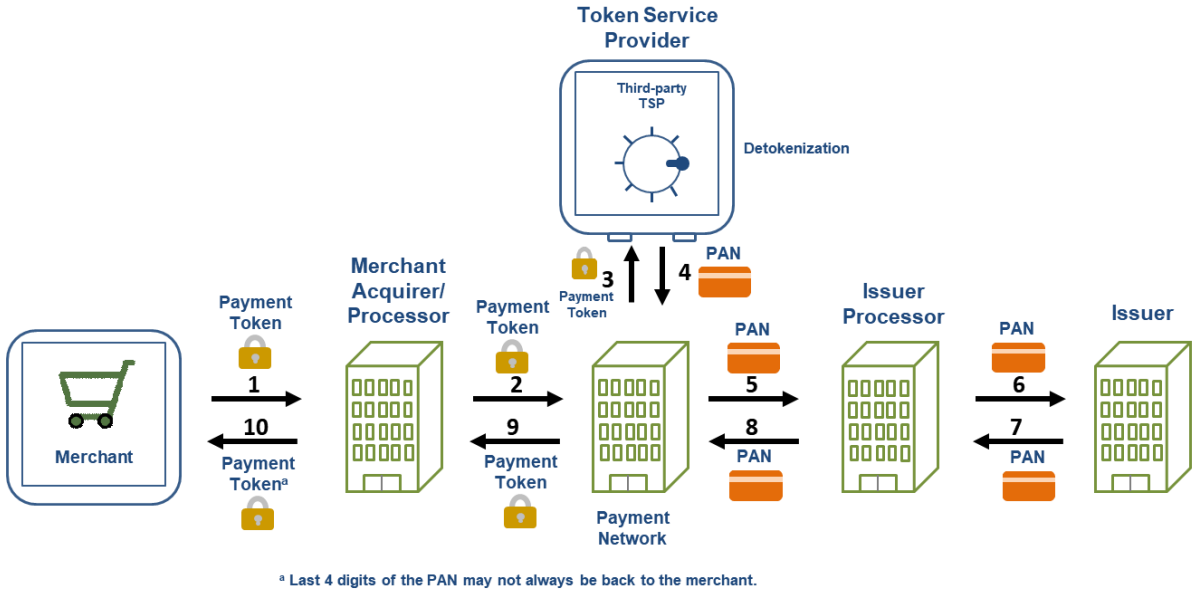


Figure 10. Process for Transactions Using a Merchant-Stored Tokenized Card (COF) Based on Third-Party TSP Tokens

During the transaction process, the following steps occur:

1. The cardholder at a merchant shopping site (or using a mobile application) elects to pay with a card previously stored on the merchant site. The transaction is initiated, and a message containing the payment token is forwarded to the merchant acquirer/processor.
2. The merchant acquirer/processor receives the transaction request and uses the token to perform a token lookup and determine the networks to which the transaction can be routed. The merchant acquirer/processor routes the transaction to the appropriate credit or debit payment network (debit based on the preferred routing choice, least cost, or some other criterion agreed to by the merchant).
3. The payment network determines that this transaction is based on a token BIN and issues a request to the appropriate TSP to detokenize the token to the clear PAN.
4. The TSP returns the clear PAN to the payment network.

5. The payment network routes the transaction to the appropriate issuer processor, based on the (token) BIN derived from the token (PAN) in the transaction.
6. The issuer processor forwards the authorization request with the clear PAN to the issuer.
7. The issuer completes the final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor responds to the merchant web site or mobile application to complete the transaction.

5.3 Transaction Processing (Network Pay Button)

Figure 11 illustrates the processing for tokenized transactions using a mobile phone with a network pay button. Note that not all transactions with pay buttons will be tokenized.

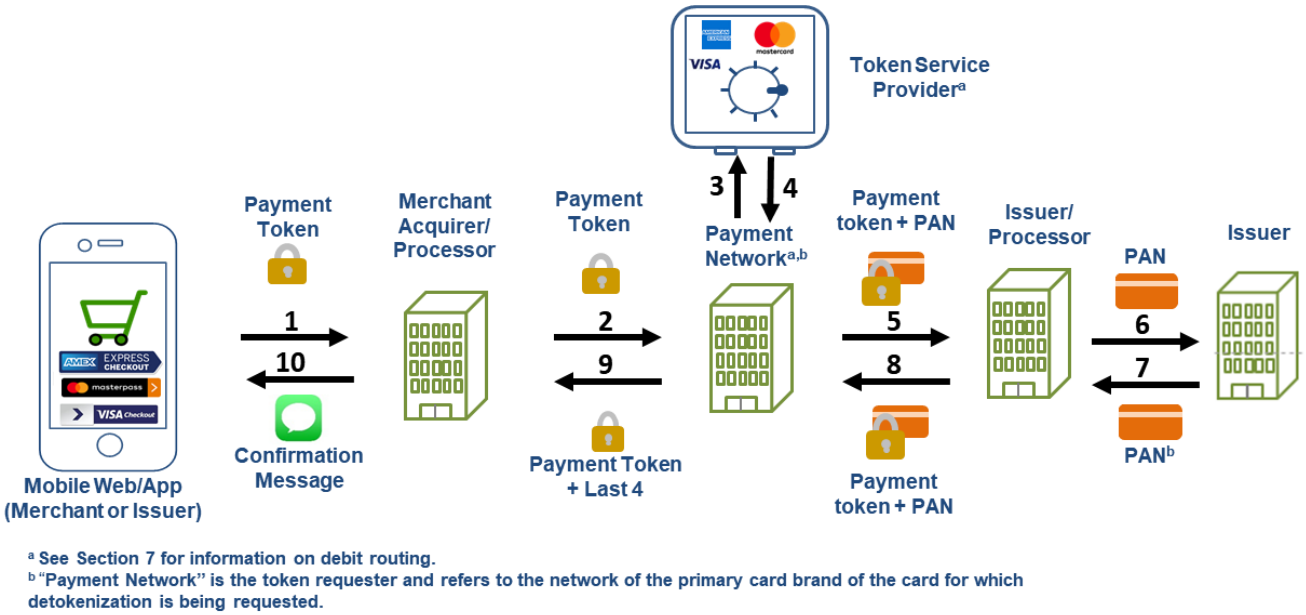


Figure 11. Transaction Using a Network Pay Button

During the transaction process, the following steps occur:

1. The cardholder uses a mobile app or web browser interface at checkout and selects to pay using a cloud-based wallet. The cardholder is redirected to the cloud wallet server for authentication. The cardholder verifies the amount and selects the token for payment. The cardholder is redirected to the mobile application or web with a payment transaction identifier.[7] The payment transaction identifier is passed to merchant's back office to complete the payment

[7] The payment transaction identifier is a unique number identifying a transaction the customer has accepted on the cloud wallet server. It does not include a token or cryptogram data.

process. The merchant's back office uses the payment transaction identifier to obtain a token and cryptogram from the cloud wallet server. The merchant's back office sends the token and cryptogram to the merchant acquirer/processor.

2. The merchant acquirer/processor routes the transaction to the appropriate payment network (based on the preferred routing choice, least cost, or some other criterion agreed to with the merchant).
3. The payment network determines that this transaction is based on a token BIN and issues a request to the appropriate TSP to validate the unique cryptogram and detokenize the token to a clear PAN.
4. The TSP verifies the cryptogram and returns the clear PAN to the payment network.
5. The payment network forwards the transaction with the clear PAN to the appropriate issuer processor.
6. The issuer processor forwards the authorization request, with the clear PAN, to the issuer.
7. The issuer completes final authorization and sends an authorization response to the issuer processor.
8. The issuer processor sends the authorization response to the payment network.
9. The payment network sends the authorization response to the merchant acquirer/processor, ensuring that the token, not the clear PAN, is included.
10. The merchant acquirer/processor sends the transaction response to the mobile application. The merchant's back office confirms payment status to the cloud wallet server.

6. Impact of Payment Tokenization on Merchants

To document the impact of payment tokenization on merchants, more than a dozen industry experts were consulted, including three large merchants, four payment networks, and two acquirers. While there appeared to be common understanding of, and agreement on, many of the negative effects of tokenization on merchants, there is a surprising amount of misunderstanding about the impact of payment tokenization on debit routing and not much consensus on workarounds or solutions.

The negative effects fall into four categories:

- Customer confusion
- Merchant processes
- Customer identification
- Transaction routing

Sections 6.1 through 6.5 review the impacts in these categories; Section 6.6 discusses workarounds to these impacts.

6.1 Customer Confusion

For more than a decade, when customers use a credit or debit card for payment, merchants have printed the last four digits of the card number on the receipt, which is generated after the authorization. Customers are very accustomed to seeing some resemblance of the PAN (i.e., "last four" digits on card) on statements, receipts, checkout pages, e-mails, payment reminders, alerts, and practically all communications related to their credit and debit cards.

In nearly all implementations of payment tokenization, the token bears no relationship to the PAN and does not preserve the last four digits. Looking at a receipt and not recognizing the last four digits, customers may think the transaction is erroneous and dispute the purchase, resulting in merchant chargebacks. Even if the customer understands the difference, only the savviest customers would know where to look to find the token (e.g., in the case of Apple Pay, the token) to match the last four digits to a receipt.

In light of the potential for customer confusion, there are ways to find and identify the last four digits of the PAN and instances where the last four digits are not relevant. These are discussed below.

A field is defined in the EMV payment tokenization specification that is returned in the authorization response that provides the actual PAN last four digits. A merchant may receive this value so that the receipt matches the PAN in cases where matching is important. Other instances include the following:

- Where receipts are not required, especially for low-value transactions, the need for the last four digits to be displayed is eliminated.
- The wallets themselves also provide an identification of the last four digits of the token.
- Most issuers have FAQs that help a consumer understand that the number of the receipt may not match. This is also typically checked if a customer disputes a transaction.
- Lastly, transaction history is typically sent to the device and serves as an alternative validation of the purchase.

6.2 Merchant Processes

Many merchants use the PAN as the identifier to look up a lost receipt in the transaction log or database. Without the PAN, this process must be changed. In addition, customers are increasingly disputing transactions, saying "that's not my card number on the receipt." The result is additional back-office burden on the merchant.

Merchants who allow customers to buy online and pick up their purchases in store use the PAN to locate the transaction. Without the PAN, the process must be changed.

6.3 Customer Identification

Some merchants use the PAN as a customer identifier for both loyalty and analytical purposes. Tokenization may negatively affect both uses.

Without a PAN, merchants may be unable to identify customers unless the merchant has a separate customer identifier (e.g., loyalty account number). This affects rewards programs, co-branded card perks and tracking, and loyalty or membership programs.

The inability to identify customers without a PAN may also affect the reliable use of analytics, both for marketing and fraud tracking. Since a customer or fraudster may be performing transactions with multiple tokens, there may not be a way to tie transactions to a single customer or fraudster. Fraud velocity-checking analytics is an issue for e- and m-commerce merchants and may be used to identify multiple attempts with a card at an in-store POS.

NOTE: Please see Section 6.6.1 discussion on PAR, which was designed to address these issues.

6.4 Transaction Routing

Tokenization can affect transactions in many ways. As noted further in Section 7, in order to ensure merchant routing choice where tokenization is used, acquirers and merchants may need to adjust processes and business practices to identify tokens and determine where they can route transactions based on rules and capabilities.

First, since 2010, U.S. merchants are entitled to choose between two unaffiliated debit networks available on the applicable card for routing debit transactions. The choice is typically between a global payment network (such as Visa or Mastercard) and one of the regional payment networks (originally known as PIN debit networks, such as PULSE or SHAZAM). Both EMV and payment tokenization introduced complexities into this routing decision (see Section 7 for more information on this topic).

Second, merchants want to choose their best routing options based on cost or other factors, which requires identifying that the transaction is tokenized. This requires the merchant or its acquirer to identify the routing options available based on the token BIN(s) present in the routing table before the authorization attempt.

However, as shown in Section 5, merchants may not be able to route certain card-on-file or card-not-present debit transactions based on payment network, where tokenization is used. Merchants are advised to consult with the payment networks for additional information.

6.5 Cardholder Verification

For a tokenized card-present transaction, TSPs don't provide all Track 2 discretionary data to the issuer. This can affect the issuer's processes for verifying the cardholder (e.g., card security code check, PIN offset) and the issuer's authorization decision.

6.6 Merchant and Issuer Impact Workarounds

The payment industry's long-term solution for most of the operational effects of tokenization is implementation of the EMV Payment Account Reference (PAR), a non-financial reference assigned to each unique PAN and used to link a payment account represented by that PAN to affiliated payment tokens.[8] When made available to stakeholders at the point of interaction, the PAR will resolve the operational issues related to linking and customer identification, but will not improve transaction routing. However, implementation of PAR requires changes coordinated among all payment ecosystem stakeholders, which will take some time (likely a number of years) to achieve. Also, PAR is not visible to cardholders and, therefore, does not solve the customer confusion issues addressed in Section 6.6.1.

In the meantime, various other workarounds have been proposed.

6.6.1 Customer Confusion and Merchant Process Issues

One approach to address customer confusion and merchant process issues is to make the last four digits of the PAN available across the ecosystem. While the EMVCo specification already has a field that carries the last four digits in the authorization return message, it is not a required field and may not be consistently populated across the entire ecosystem.[9]

The U.S. Payments Forum recommends making the last four digits of the PAN available across the ecosystem as quickly as feasibly possible. If the last four digits are returned to the acquirer, they should be passed along to the merchant so that they can be used.

In the current tokenized world, there is no reference number on the receipt to tie a receipt to an account. Only the last four digits of the token are on the receipt and cardholders may not know how to find the card number tied to the token number. Unless this changes, a household with multiple accounts with several members of the household having access to more than one account and several members doing transactions with both cards and mobile devices cannot easily tie a receipt to its applicable account and statement.

Wallets which support tokens today do provide the user with a transaction history, provided by the issuer that allow the consumer to understand which purchases they made from the unique device.

---

[8] EMVCo, "EMV® Payment Tokenisation Specification – Technical Framework," Sept. 8, 2017, and Secure Technology Alliance, "EMVCo Payment Account Reference (PAR): A Primer," April 2018.

[9] Mastercard provides the full PAN to acquirers for tokenized transactions in ISO messaging DE 48 Sub-element 33. However, acquirers may not be passing the last four digits to the merchant; Mastercard has not created a best practice for acquirers to share the last four of a PAN as of yet. Visa uses field 4415, which is the last four digits of the PAN. Discover enabled the passage for the last four digits of the PAN when it updated its ISO in 2015 to support EMV tokens. The last four digits of the PAN can be found in Field 106 (Transactional Data), Data set 61 (Payment Token Data), Tag 1.

This may make reconciliation difficult and time consuming and may increase calls to both issuer and merchant call centers. To further help address these concerns, issuers may wish to consider educating cardholders about how to locate the last four digits of the token number on devices and providing other means of identifying the account debited or credited by a transaction. This might include printing the current last four digits of each account's tokens on each statement or it might include providing an on-line look-up feature for the last four digits of the token through the issuer's web site. These options will be especially important for transactions done with a tokenized card and no device.

Even when the last four digits of the PAN are available, the ability to print them on the receipt can be limited by whether the receipt printing process is a respond receipt or a receive receipt. Respond receipts are created upon transaction response, so the last four digits are available if the field has been populated. In contrast, read receipts, which are more typical among larger merchants, are created based on data read from the POS device before the authorization response has been received; in this case, the last four digits are not available.

Though paper receipts still dominate at the POS, over time they will be replaced by electronic receipts similar to those in the ecommerce environment. It is possible to insert the last four digits into an electronic receipt after the receipt is initially created.

Another approach employed by some large merchants to accommodate customer service for tokenized transactions is to look up in-store or e-commerce transaction receipts or order identifiers. If the customer can supply the date, approximate time of day, and transaction amount (from a credit card statement or wallet transaction history) and identify the POS (in the case of an in-store purchase), a transaction log can be manually searched to find the receipt. Often the order identifier is the better option.

As PAR becomes available,[10] merchants can start capturing the PAR from the acquirer's response (if the acquirer is providing it). The networks are providing a PAR-lookup API service. The merchant can use this API to obtain the PAR and match it in the transaction log.[11]

Customers who order online and pick up the order in the store should be able to retrieve the order identifier from the online account.

6.6.2 Customer Identification

The alternative to using PANs for customer identification is to use a separate loyalty account number, e-mail address, or telephone number.

6.6.3 Cardholder Verification

Issuers may wish to implement host-based PINs for cardholder verification with tokenized card-present transactions. Issuers do not need to check the card security code (e.g., CSC, CVV, CID) but rely on the dynamic cryptogram validation by the TSP.

[10] As of June 2018, some global networks have begun to enable PAR for tokenized credentials only.

[11] Some merchants admit to having lax return and refund policies and process returns or refunds without a receipt for the sake of customer experience.

7. Merchant Debit Transaction Routing

Tokenization may affect debit routing for some payment networks in several situations: when the transaction is a proximity POS transaction made using EMV payment tokens, and when the transaction is made using a card on file, in-app, or as part of a pay button. Routing may also be impacted based on the tokenization solution implementation.

7.1 Contactless POS Transactions with EMV Payment Tokens

Merchants are able to choose the routing for contactless EMV debit transactions[12] made from a mobile device when U.S. Common Debit AID is selected, as long as the debit payment network connects with a TSP to detokenize transactions before processing. If a Global AID is selected, the debit transaction can only be routed to the global network.

Some payment applications have implemented the U.S. Common Debit AID without support for the Consumer Device Cardholder Verification Method (CDCVM).[13] In these cases, the transaction is passed to the debit payment network marked "No CVM." With No CVM, while the merchant's routing choice is preserved, the merchant may be exposed to chargeback liability for lost-or-stolen transactions unless online PIN is captured.[14]

7.2 Merchant Card on File

Some merchants elect to replace COF credentials with COF payment tokens. If the merchant elects this option, some global payment networks require that merchants route tokenized COF transactions to their respective networks only, when the COF token was issued by their TSP.

Similar routing limitations apply to tokenized in-app and pay button solutions for certain global networks. This can impact merchant routing to unaffiliated debit networks.

Current approaches to routing options are varied. Contact the payment networks for policies on routing tokenized transactions.

[12] MSD contactless transactions work differently and is out of scope for this paper.
[13] CDCVM uses a passcode or biometric on the mobile device.
[14] U.S. Payments Forum, "PIN Bypass in the U.S. Market," February 2019.

8. Conclusions

This white paper examined the use of tokenization as a tool to protect payment card data and reduce the opportunity for using card data for fraudulent purposes. Tokenization provides an important layer of payment security but also has implementation considerations across the ecosystem.

This paper focuses on the state of payment tokenization today, providing the reader with an understanding of payment tokenization, the payment scenarios in which tokenization can be used, and the services that are commonly used in payment tokenization. The paper describes common token processing flows and discusses the impact of payment tokenization on merchants.

It is hoped that the information in this paper will help organizations make informed decisions on tokenization and determine how it fits into their payment security strategy.

9. Legal Notices

While great effort has been made to ensure that the information in this document is accurate and current as of the publication date, this information does not constitute legal advice and should not be relied upon for any legal purpose, whether statutory, regulatory, contractual or otherwise. Any person that uses or otherwise relies in any manner on the information set forth herein does so at his or her sole risk. All warranties of any kind, whether express or implied, relating to this document, the information set forth or otherwise referenced herein or the use thereof are expressly disclaimed, including but not limited to all warranties relating to or arising in connection with the use of or reliance on the information set forth herein, all warranties as to the accuracy, completeness or adequacy of such information, all implied warranties of merchantability and fitness for a particular purpose, and all warranties regarding title or non-infringement.

Merchants and others implementing tokenization are strongly encouraged to consult with their respective payment networks, acquirers, processors and appropriate professional and legal advisors regarding all aspects of implementation.

Without limiting the foregoing, it is important to note that the information provided in this document is limited to the specific matters expressly described herein.

Nothing in this document constitutes or should be construed to constitute an endorsement or recommendation by the U.S. Payments Forum of any particular approach, service or provider, and all implementation decisions and activities should be properly reviewed in light of applicable business needs, strategies, requirements, industry rules, and laws.

Publication of this document does not imply the endorsement of any U.S. Payments Forum member organization.

10. Glossary

Acquirer. The party recognized by the network as the financial sponsor for a merchant (typically a regulated financial institution, such as a bank). The acquirer supports the merchant by providing the connection to payment networks to process purchase authorizations based on tokenization. The acquirer may possibly play the role of a token requestor in support of the card-on-file payment scenario.

Application Program Interface (API). Code that allows two software programs to communicate with each other.

Account Updater. Service provided to merchants by most payment networks to update accounts for merchants who store cards on file. These PANs are kept for cardholders to generate new or recurring payment transactions. The account updater services update lifecycle information about the PANs on file, allowing merchants to continue to transact with little interruption.

Bank Identification Number (BIN). The first six or eight digits of a payment card number (e.g., credit cards, debit cards). These are now known as the Issuer Identification Number (IIN). The BIN/IIN identifies the institution that issued the card to the cardholder.

Cardholder Verification Method (CVM). In the context of a transaction, the method used to authenticate that the person presenting the card is the valid cardholder.

Card on File (COF). Payment credentials provided by the cardholder to a merchant with the authorization to use the stored credentials for individual or recurring payment. Stored payment credentials are provided by a cardholder to a specific retailer's online or mobile application.

Cloud. A reference to using cloud computing to access services and applications. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Contactless Payments. Payment transactions that require no physical contact between the consumer payment device and the physical terminal. In a contactless payment transaction, the consumer holds the contactless card, device, or mobile phone in close proximity (less than 2-4 inches) to the terminal and the payment account information is communicated wirelessly (via radio frequency [RF]) or NFC.

Digital Wallet. A software representation of a physical wallet; for example, putting debit and credit cards into an application that holds payment credentials through which someone can pay, using the digital version of the debit or credit cards in that person's physical wallet and linking to the same account. Applications housed on mobile devices such as smartphones are used to initiate a transaction with the device itself. To reduce the risk of data theft from the device or application, wallets do not store sensitive credentials for long term use but replace the consumer's payment credentials with non-sensitive token values through an established out-of-band enrollment process with the consumer's card issuer. Digital wallets can store consumer's payment credentials in different ways, either through hardware-based or software-based applications.

Host Card Emulation (HCE). Mechanism for an application running on the "host" processor (the mobile device's main processor where most consumer applications run) to perform NFC card emulation transactions with an external reader. Examples of HCE implementations include the Android operating system (Android KitKat 4.4 and higher) and the BlackBerry operating system.

Identification and Verification (ID&V) Process. The process to ensure that the legitimate cardholder that was issued the PAN by the issuer is interacting with the token requestor during the request for a payment token. This involves the verification of the previously-established identity of the cardholder.[2]

In-App Payment. Making a mobile purchase from within a mobile app. There is a distinction between paying with NFC-enabled mobile wallets and paying directly through the merchant-specific native mobile app with a credit, debit or prepaid card number, typically stored in a digital wallet.

Internet of Things (IoT). A system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-compute

Issuer. A financial institution that provides cardholders with payment accounts represented by one or more PANs. The issuer is responsible for approving payment tokens through the ID&V process. The issuer will also authorize transactions using payment tokens.

Issuer Processor. An entity that facilitates card issuance activities on behalf of an issuer such as processing payment transactions, enrolling cards, preparing and sending the card personalization information to the card vendor, and maintaining the cardholder database.

Magnetic Secure Transmission (MST). A proprietary technology implemented in certain mobile phones that uses RF to communicate payment account information with a magnetic-stripe reader of a POS terminal.[1]

Magnetic Stripe Data (MSD). A contactless payment transaction that transfers data that is formatted as the magnetic stripe of a credit or debit card.

Merchant. Entity that accepts payments from customers in exchange for goods and/or services and connects to a payment network through an acquirer. Merchants request authorization of transactions using tokens as the payment credential. Merchants possibly play the role of a token requestor in support of the COF payment scenario.

Mobile Wallet. The mobile version of a digital wallet, provisioned and accessed on a mobile device.

Near Field Communications (NFC). A set of standards that enables proximity-based communication between consumer electronic devices such as mobile phones, tablets, personal computers or wearable devices. An NFC-enabled mobile device can communicate with a POS system that accepts contactless EMV payment cards.

Pay Button. Branded online checkout tools on the retailer's web site or mobile app that are used to perform consumer-initiated transactions. Pay buttons can be in the form of branded digital wallets using credit, debit, and/or alternative payments. While digital wallets reside within an application on the customer's device, pay buttons are embedded within the retailer's ecommerce checkout page or mobile application, and can be accessed by the consumer from a mobile device, tablet, or PC.

Payment Account Reference (PAR). A non-financial reference assigned to each unique PAN and used to link a payment account represented by that PAN to affiliated payment token.[2] As multiple payment tokens can be associated to the same underlying PAN, the PAR is a non-financial token value that has a one-to-one relationship with the underlying PAN assigned to help enable identification of the customer for backend processes such as loyalty tracking. The PAR cannot be used for financial transactions (e.g., authorization requests, settlement, reversals).

Payment Network. The entity providing POS and ATM services for credit, debit, ATM and prepaid card issuers and corresponding transaction acquirers. The payment network establishes participation requirements, operating rules and technical specifications under a common brand(s) for the purpose of receiving, routing, securing authorization for, settling and reporting domestic and international payment transactions. Each payment network determines the types of transactions, payment devices and terminals that are permitted in its respective network. The payment network connects merchants, acquirers, processors, and issuers in order to authorize payment token transactions. Payment networks also typically play the role of a token service provider.

Payment Token. A surrogate value for a PAN that is a variable length, ISO/IEC 7812-compliant numeric issued from a designated token BIN or token BIN range and flagged accordingly in all appropriate BIN tables. A payment token must pass basic validation rules of a PAN, including the Luhn check digit. Payment tokens must not collide or conflict with a PAN.[(2)]

Payment Tokenization. A specific form of tokenization whereby payment tokens are requested, generated, issued, provisioned, and processed as a surrogate for PANs.[(2)]

Point-of-Sale (POS). The device (hardware and software) that is used to process transactions at the merchant location. While POS once referred specifically to the credit card terminal at the cash register, POS now includes mobile, wireless, and virtual terminals.

Primary Account Number (PAN). A variable length, ISO/IEC 7812-compliant account number that is generated within account ranges associated with a BIN by an issuer.[(2)]

Provisioning. An initial set up process that handles authentication of a user account, the exchange of keys to unlock the NFC chip installed on a mobile device, the service activation and the secure download of mobile payment account information.

Secure Element. A hardware function residing in a microcontroller chip capable of performing cryptographic operations. It offers a dynamic environment to store data securely, process data securely and perform communication with external entities securely. If tampered with, it may self-destruct, but will not allow unauthorized access.

Third-party TSP. An entity that isn't a payment network that provides tokenization services, including token vault management.

Token. Generic term for a placeholder or surrogate. In the context of payment card transactions, a token refers to a surrogate card number that is submitted in the payment stream in place of the real card number.

Token BIN. A specific BIN that has been designated only for the purpose of issuing payment tokens and is flagged accordingly in BIN tables.[(2)]

Token BIN Range. A specific BIN range that has been designated only for the purpose of issuing payment tokens and is flagged accordingly in BIN tables.[(2)]

Token Cryptogram. A cryptogram, containing a transaction-unique value, typically generated using the payment token, payment-token-related data, and transaction data. Cryptogram derivation methods may vary by scenario and may be payment system specific.

Token Domain Restriction Control. A set of parameters established as part of issuing a payment token that will allow enforcement of appropriate usage of the payment token during processing.[(2)] Issuers have the responsibility to set token domain controls for use of the token.

Tokenization. Process by which a placeholder or surrogate (token) is substituted for a PAN. Typically, tokenization is a service offered by a payment network, acquirer, token service provider or third-party service provider.

Token Requestor. Entity that initiates requests that PANs be replaced with non-sensitive tokens for long-term storage and future use by submitting token requests to the token service provider.

Token Requestor Identifier (TRID). An 11-digit numeric value that identifies each unique combination of token requestor and token domain(s) for a given token service provider.[(2)]

Token Service Provider (TSP). Entity within the payments ecosystem that provides registered token requestors with 'surrogate' PAN values, otherwise known as payment tokens by managing the operation and maintenance of the token vault, deploying security measures and controls, and providing a registration process of allowed token requestors.

Token Vault. A secure Payment Card Industry (PCI)-compliant server where tokens are issued, and the PAN numbers they represent, are stored securely.

Wallet Service Provider. Companies that offer specific wallet solutions that use various communications technology for mobile payments.

Wearable. In the context of payment, relating to or noting a computer or advanced electronic device that is incorporated into an accessory or item of clothing worn on the body.

White Box Cryptography. A technology that allows cryptographic operations to be performed without revealing any portion of confidential information such as the cryptographic key[15].

[(1)] Source: U.S. Payments Forum Mobile and Contactless Payments Glossary

[(2)] Source: EMVCO EMV Payment Tokenization Specification Technical Framework v2.0

[15] Source: White-box Cryptography